

EXHIBIT A

Search Warrant

UNITED STATES DISTRICT COURT

for the
District of DelawareIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
511 DANIELS COURT, BEAR,
DELAWARE 19701)
)
)
)
)
)

Case No. 20 - 250M

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Delaware
(identify the person or describe the property to be searched and give its location):


See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B-1

YOU ARE COMMANDED to execute this warrant on or before October 20, 2020 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ a U.S. Magistrate Judge
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: October 6, 2020 at 5:45 p.m.
Judge's signatureCity and state: Wilmington, DelawareU.S. Magistrate Judge Christopher J. Burke
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

[illegible]

ATTACHMENT A
Property to Be Searched

The location to be searched (“**TARGET PREMISES**”) is identified and described as follows: a residential structure located at 511 Daniels Court, Bear, Delaware 19701. It is a one-story house with the exterior consisting of light gray colored siding. There is a one-car garage on the right-hand side of the residential structure with a white front door in the middle of the structure. The backyard of the resident is surrounded by a white, approximately three-foot tall privacy fence. Contained within the white fence are two sheds. One is yellowish with a brown roof and the other is light gray with a dark colored roof.

Photographs of the **TARGET PREMISES** and the adjacent sheds are pictured below:





ATTACHMENT B

Items to be Seized from Property Described in Attachment A

All items and records, in whatever form they exist, that constitute evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 1201(c) (“TARGET OFFENSE”), including but not limited to:

1. Firearms, firearm equipment, and ammunition of any kind;
2. Any edged weapons, including by not limited to: tomahawks, knives, and swords;
3. Records regarding the purchase, assembly, or storage of firearms, ammunition, or other weapons;
4. Records regarding the purchase, assembly, or storage of energetic material and other components used in the construction of an Improvised Explosive Device, including but not limited to: silicone bottles, black powder, smokeless powder, propane tanks, hobby fuse, adhesives, duct tape, and BBs or other hardened material;
5. Components used in the construction of an Improvised Explosive Device, including but not limited to: silicone bottles, black powder, smokeless powder, propane tanks, hobby fuse, adhesives, duct tape, and BBs or other hardened material;
6. Any books, literature or other materials related to instructions about how to build explosive devices;
7. Tactical gear, including but not limited to: body armor, fatigues, trail cameras, and handheld radios;
8. Any illegal drugs, including but not limited to marijuana, or materials used to process/distribute illegal drugs;
9. Any and all materials such as literature, paraphernalia, clothing, or membership in organizations, such as, but not limited to, the “Bugaloo Boys” and the “Three Percenters”;
10. Records related to any other storage facilities owned or controlled by CROFT;
11. Appointment books, diaries, calendars, maps, phone numbers, email addresses, and real property addresses;
12. Records related to an hotel stays in Dublin, OH; Portage, WI; Peebles, OH; Big Rapids, MI;

13. Any and all photographs, including still photos, negatives, video recordings, depicting the activity related to making or building explosive devices, firearms, or the use of any explosive devices or firearms;
14. Cellular telephones or other mobile electronic devices which could contain the following:
 - a. Evidence of purchases of explosive making materials
 - b. Names and contact information of co-conspirators
 - c. Evidence of communication with co-conspirators through voice call, email, text messaging and instant messaging and other cellular telephone communication applications;
15. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to the TARGET OFFENSE. The following definitions apply to the terms as set out in this affidavit and attachment:
 - a. Computer hardware: Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
 - b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
 - c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.
 - d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually

operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

16. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant.
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;
 - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- i. contextual information necessary to understand the evidence described in this attachment.
17. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):
- a. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
 - b. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
 - c. “scanning” storage areas to discover and possibly recover recently deleted files;
 - d. “scanning” storage areas for deliberately hidden files; or
 - e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

If it is determined that one or more of the electronic devices can be enabled with “Touch ID,” law enforcement officers will be authorized to press the fingers (including thumbs) of CROFT to the Touch ID sensor of the electronic device, for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by these warrants. Law enforcement will not use force to effect this biometric authorization, and will instead explain the warrant’s requirement to the individual in order to gain compliance.

If determined that one or more of the electronic devices can be enabled with facial recognition, law enforcement officers will be authorized to hold the device to the face of CROFT for the purpose of attempting to unlock the device via facial recognition in order to search the contents as authorized by these warrants.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities

described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

With respect to the electronic devices and COMPUTER equipment, law enforcement may seize all data and information on the devices and equipment but is authorized to look for evidence, fruits, contraband, and instrumentalities regarding the TARGET OFFENSE only from January 1, 2020, through the present.